CLAIMS

1. An electronic identification system comprising:
   - a plurality of transponders;
   - at least one transponder encoder for writing respective first watermark data into a memory arrangement of each transponder;
   - at least one verifier for interrogating a selected transponder and to read data stored in the transponder;
   - said first watermark being derived from an algorithm and input data;
   - the verifier comprising computing means configured to retrieve the algorithm and the input data and to compute second watermark data for comparison with the first watermark data.

2. An electronic identification system as claimed in claim 1, wherein the algorithm is an encryption algorithm and the input data is at least one of a constant and a variable.

3. An electronic identification system as claimed in claim 1 or claim 2, including at least one reader for reading the data transmitted, the reader not comprising the computing means configured as aforesaid.

4. An electronic identification system as claimed in any one of claims 1 to 3, wherein said at least one verifier is used for verification of the authenticity of a transponder and said at least one reader is merely for reading data transmitted by the transponder when interrogated.

5. An electronic identification system as claimed in any one of claims 1 to 4, wherein the data transmitted by the transponder comprises the first watermark data and identification code data associated with the transponder.

6. An electronic identification system as claimed in claim 5, wherein said at least one verifier utilizes said identification code data to retrieve the algorithm and the input data from memory means of the verifier.

7. An electronic identification system as claimed in claim 6, wherein at least part of the input data is alternatively or in addition derived from sensor means response to a parameter of the response signal or a communications channel with the transponder.

8. A method of authenticating a transponder of an electronic identification system, the method comprising the steps of:

- writing into a memory arrangement of the transponder first watermark data derived from an algorithm and input data for the algorithm;
- interrogating the transponder by causing the transponder to transmit to a verifier a response signal comprising data stored in the memory arrangement of the transponder;
- utilizing at the verifier the transmitted data to retrieve the algorithm and the input data;
- utilizing the retrieved algorithm and input data to compute second watermark data; and
- comparing the first watermark data and the second watermark data to give an indication of the authenticity of the transponder.

9. A method as claimed in claim 8, wherein the first watermark data is generated by an encoder and is written into the memory arrangement of the transponder.

10. A method as claimed in claim 8 or claim 9, wherein the encoder is connectable to a central station for downloading into a memory arrangement of the encoder a set of algorithms comprising said algorithm.

11. A method as claimed in claim 10, wherein the central station and/or encoder are further configured to write the set of algorithms and

input data for the set of algorithms into a memory arrangement of the verifier.

12. A method as claimed in any one of claims 8 to 11, wherein said algorithm and said input data for said algorithm are stored in the verifier in relation to identification code data of the transponder.

13. A method as claimed in any one of claims 8 to 12, wherein the input data is arbitrarily selected data and is changed by the encoder from time to time.

14. A method as claimed in any one of claims 8 to 13, wherein the data transmitted to the verifier in the response signal comprises identification code data of the transponder.

15. A method as claimed in claim 14, wherein the identification code data is utilized by the verifier to retrieve said algorithm and said input data.

16. A method as claimed in any one of claims 8 to 15, wherein the input data for said algorithm further comprises data derived by the verifier from a parameter of said response signal or a communications channel with the transponder.

17. A method as claimed in any one of claims 8 to 16, wherein the step of comparing the first watermark data and the second watermark data is performed on the verifier, the first watermark data being transmitted by the transponder to the verifier.

18. A method as in any one of claims 8 to 16, wherein the step of comparing the first watermark data and the second watermark data is performed on the transponder, the second watermark data being computed on the verifier and then transmitted to the transponder where the comparison is performed, the transponder then providing the indication of the authenticity of the transponder.

19. A verifier for authenticating a transponder, comprising a transmitter for transmitting an interrogation signal to the transponder, a receiver for receiving a response signal from the transponder, the response signal carrying or embodying ID code data of the transponder, a controller for utilizing the ID code data to retrieve from a memory arrangement an algorithm and input data associated with the transponder, and processing means for deriving computed watermark data from the retrieved algorithm and associated input data.

20. A verifier as claimed in claim 19, wherein the verifier is arranged to transmit the computed watermark data to the transponder for

comparison with stored watermark data stored within the memory of the transponder.

21. A verifier as claimed in claim 19, wherein the verifier is arranged to compare the computed watermark data with stored watermark data in the memory arrangement of the verifier.

22. A verifier as claimed in any one of claims 19 to 21, wherein the retrieved algorithm is an encryption algorithm and the retrieved input data is at least one of a constant and a variable.

23. A transponder for use in an electronic identification system, comprising a transmitter for sending a response signal to a verifier, the response signal carrying or embodying ID code data of the transponder, a receiver for receiving from the verifier computed watermark data derived from a retrieved algorithm and associated input data in the memory arrangement of the verifier, and processing means for comparing the computed watermark data with stored watermark data stored within the memory of the transponder, to establish authentication of the transponder.

24. A transponder as claimed in claim 23, arranged to transmit an authenticity signal to the verifier indicative of the authenticity or otherwise of the transponder.